ELSEVIER

Journal of Pure and Applied Algebra 113 (1996) 219–227

JOURNAL OF PURE AND APPLIED ALGEBRA

Polynomials and radical ideals

B. Banaschewski*, J.J.C. Vermeulen

Department of Mathematics, University of Cape Town, Rondebosch 7700, South Africa

Communicated by P.T. Johnstone; received 4 January 1994; revised 2 October 1995

1991 Math. Subj. Class.: 13A10, 13B25, 54H99

0. Introduction

The familiar result that, over any commutative ring A with unit, the product of primitive polynomials is primitive is usually proved by taking a prime ideal containing the coefficients of the product and then deriving a contradiction. This argument, depending on the Axiom of Choice (or more precisely, on the Prime Ideal Theorem for Boolean algebras) and the Law of the Excluded Middle, poses the obvious question whether the result is already constructively valid (in the usual sense of Topos Theory).

As a natural approach to this, one might try to bypass the putative existence of prime ideals by using the propositional geometric theory of a prime instead. This led us to consider, for any polynomial $u \in A[x]$, the radical ideal $J(u)$ generated by its coefficients, which we call the *radical content* of u. For this, we first establish the crucial identity $J(uv) = J(u) \cap J(v)$ (Proposition 1) and then show how that leads to simple proofs of various familiar facts, including the result in question on primitive polynomials. Next, we give an alternative proof of our identity which makes the connection with the theory of a prime more transparent (Section 2), and then deal with its significance for the localic spectra of A and $A[x]$ (Proposition 2). Finally, we consider the obvious generalization of the radical content on monoid algebras $A[M]$ for decidable commutative monoids M, characterizing those M for which the crucial identity is satisfied (Proposition 3) and determining the logical relationship between several natural conditions involving the radical ideals of A and $A[M]$.

*Corresponding author. Current address: Department of Mathematics, McMaster University, 1280 Main Street, Hamilton, Ont., Canada L8S 4K1.

SSDI 0022-4049(95)00149-2

1. The radical content

In the following, A is always a commutative ring with unit 1 and $A[x]$ the ring of polynomials over A in one indeterminate x. Recall that A is called *semiprime* whenever $a^n = 0$ implies $a = 0$, for all $a \in A$.

Lemma. *If A is semiprime then, for any $u = a_0 + a_1 x + \cdots + a_n x^n$ and $v = b_0 + b_1 x + \cdots + b_m x^m$ in $A[x]$, $uv = 0$ implies that all $a_i b_k = 0$.*

Proof. We proceed by induction on $l = i + k$, the case $l = 0$ being obvious. Assuming $a_s b_t = 0$ for all $s + t < l$, consider any i, k such that $i + k = l$. Then

$$a_i b_k = - \sum_{s<i \text{ or } t<k,\, s+t=l} a_s b_t$$

implies that

$$(a_i b_k)^2 = - \sum_{s<i \text{ or } t<k,\, s+t=l} a_s b_k a_i b_t = 0$$

since $s + k < l$ or $i + t < l$. □

Next, we use this lemma to obtain a result for arbitrary A.

For any polynomial

$$u = a_0 + a_1 x + \cdots + a_n x^n$$

in $A[x]$, we put

$$J(u) = \operatorname{rad}(a_0, a_1, \ldots, a_n) = [a_0, a_1, \ldots, a_n],$$

where $\operatorname{rad} I = \{s \in A \mid \text{some } s^n \in I\}$ is the usual radical ideal for any ideal I and $(a_0, a_1, \ldots, a_n)$ is the ideal generated by $a_0, a_1, \ldots, a_n$. We consider $J(u)$ as a generalization of the usual content of a polynomial over $\mathbb{Z}$ and call it the *radical content* of u.

Now, for any u as above and any further polynomial $v = b_0 + b_1 x + \cdots + b_m x^m$,

$$J(u) \cap J(v) = [a_0, a_1, \ldots, a_n] \cap [b_0, b_1, \ldots, b_m] = [a_0 b_0, \ldots, a_i b_j, \ldots, a_n b_m] \quad (*)$$

the latter since $s^k \in (a_0, a_1, \ldots, a_n)$ and $s^l \in (b_0, b_1, \ldots, b_m)$ obviously implies

$$s^{k+l} \in (a_0, a_1, \ldots, a_n) \cdot (b_0, b_1, \ldots, b_m) = (a_0 b_0, \ldots, a_i b_j, \ldots, a_n b_m).$$

Then, we have the fundamental

Proposition 1. *For any $u, v \in A[x]$, $J(uv) = J(u) \cap J(v)$.*

Proof. For $\bar{A} = A/J(uv)$, let $a \rightsquigarrow \bar{a}$ be the quotient homomorphism $A \to \bar{A}$, and $\bar{u}$ and $\bar{v}$ the polynomials in $\bar{A}[x]$ corresponding to u and v. Then $\bar{u}\bar{v} = \overline{uv} = 0$, hence by the lemma all $\bar{a}_i \bar{b}_k = 0$ since $\bar{A}$ is semiprime, and therefore all $a_i b_k \in J(uv)$. By $(*)$ this shows $J(u) \cap J(v) \subseteq J(uv)$, the non-trivial inclusion. □

Remark. Proposition 1 may also be obtained as a consequence of what some authors call the Dedekind–Mertens Lemma, by which the ideals $I(u)$ generated by the coefficients of the polynomials $u \in A[x]$ satisfy the condition

$$I(u)^{m+1} I(v) = I(u)^m I(uv)$$

for any non-zero u and v, and $m = \deg(v)$. Since $J(u) = \operatorname{rad} I(u)$, and $\operatorname{rad}(HK) = \operatorname{rad} H \cap \operatorname{rad} K$ for any ideals H and K of A, this identity yields $J(u) \cap J(v) \subseteq J(uv)$, the non-trivial inclusion. For a proof of the present lemma see [8]. We note that our proof above, as well as the alternative version presented below, are fundamentally different.

We conclude by deriving some well-known results from this proposition (see [1]).

Corollary 1. *For any $u, v \in A[x]$, uv is primitive whenever u and v are primitive.*

Proof. $w \in A[x]$ is primitive iff $J(w) = (1)$. □

Corollary 2. *If A is an integral domain then so is $A[x]$.*

Proof. If $uv = 0$ in $A[x]$ then $J(u) \cap J(v) = J(0) = [0] = (0)$ and hence $J(u) = (0)$ or $J(v) = (0)$ so that $u = 0$ or $v = 0$, using in both steps that A is an integral domain. □

Corollary 3. *If A is semiprime then so is $A[x]$.*

Proof. If $u^n = 0$ for $u \in A[x]$ then $J(u) = J(u^n) = [0]$, and $[0] = (0)$, since A is semiprime, so that $u = 0$. □

Corollary 4. *For any radical ideal I of A, $I[x]$ is a radical ideal of $A[x]$.*

Proof. In any ring, and ideal is a radical ideal iff the corresponding quotient is semiprime. Hence $A[x]/I[x] \cong (A/I)[x]$ is semiprime by the preceding corollary, and this proves the result. □

Remark 1. Besides the polynomial ring $A[x]$ over A, one has the ring $A[[x]]$ of formal powers series in one indeterminate x over A. Since multiplication in $A[[x]]$ is given by

$$\left(\sum a_n x^n\right)\left(\sum b_n x^n\right) = \sum c_n x^n,$$

where

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0,$$

the inductive argument proving the lemma applies equally well here. Hence, defining $J(u)$ again as the radical ideal generated by the coefficients of u, one obtains Proposition 1 and its corollaries for $A[[x]]$.

Remark 2. An obvious induction proves the lemma, and hence Proposition 1 and its corollaries, for the natural extension of the notion of radical content to polynomial rings in any finite number of indeterminates (and consequently also for the case of an arbitrary set of indeterminates, provided it has decidable equality).

2. An alternative proof

There is a natural variant of the above proof of Proposition 1 which avoids the preliminary stage of the lemma by operating directly at the level of radical ideals, as follows:

For u and v as above, letting

$$uv = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m},$$

it has to be shown that

$$[a_i b_k] \subseteq [c_0, c_1, \ldots, c_{n+m}]$$

for all i, k. This is again done by induction on $l = i + k$, the case $l = 0$ being obvious. Assuming the condition for all $a_s b_t$ where $s + t < l$, consider any i, k such that $i + k = l$. Then

$$a_i b_k = c_l - \sum_{s<i \text{ or } t<k, s+t=l} a_s b_t,$$

hence, in the lattice of radical ideals of A,

$$\begin{aligned}[a_i b_k] &\subseteq [c_l] \vee \bigvee \{[a_s b_t] \mid s < 1 \text{ or } t < k, s + t = l\} \\ &\subseteq [c_l] \vee \bigvee \{[a_s] \mid s < i\} \vee \bigvee \{[b_t] \mid t < k\}\end{aligned}$$

and by intersecting with $[a_i b_k]$, using distributivity,

$$\begin{aligned}[a_i b_k] &\subseteq [c_l] \vee \bigvee \{[a_s b_k] \mid s < 1\} \vee \bigvee \{[a_i b_t] \mid t < k\} \\ &\subseteq [c_0, c_1, \ldots, c_{n+m}]\end{aligned}$$

the last step by induction hypothesis.

This proof has an interesting interpretation which we now describe. Recall that the propositional theory of a *prime* (complement) P of the ring A ([7]; for the notion of prime as such, see [6]) is given by the primitive propositions $a \in P$, corresponding to the elements of A, and the axioms

$$ab \in P \vdash\dashv a \in P \wedge b \in P,$$

$$true \vdash 1 \in P,$$

$$a + b \in P \vdash a \in P \vee b \in P,$$

$$0 \in P \vdash false.$$

Then, Proposition 1 may be viewed as saying that the propositional theory of a prime of $A[x]$ is modelled in the corresponding theory for A by the definition

$$u \in Q \vdash\dashv a_0 \in P \vee a_1 \in P \vee \cdots \vee a_n \in P$$

for $u = a_0 + a_1 x + \cdots + a_n x^n$: it expresses the crucial part that

$$u \in Q \wedge v \in Q \vdash uv \in Q,$$

that is,

$$(a_0 \in P \vee \cdots \vee a_n \in P) \wedge (b_0 \in P \vee \cdots \vee b_m \in P) \vdash c_0 \in P \vee \cdots \vee c_{n+m} \in P$$

for all i and k. We note further that the present proof of this is nothing but a careful reworking of the usual argument that, for any prime ideal $\mathfrak{p}$ of A, $uv \notin \mathfrak{p}[x]$ whenever $u \notin \mathfrak{p}[x]$ and $v \notin \mathfrak{p}[x]$. Thus, our alternative proof of Proposition 1 is essentially the same as a familiar proof concerning polynomials and prime ideals, albeit lifted from the usual context to that of the theory of a prime.

We conclude with a formally different but equivalent interpretation of Proposition 1. Recall that the models of the theory of a prime of A, in the bounded distributive lattice L, are the maps $\sigma: A \to L$ which (allowing a to replace $a \in P$) turn the logical terms of the theory into their lattice counterparts such that

$$\begin{aligned}
&\sigma(ab) = \sigma(a) \wedge \sigma(b),\\
&\sigma(1) = e,\\
&\sigma(a + b) \leq \sigma(a) \vee \sigma(b),\\
&\sigma(0) = 0
\end{aligned}$$

(e being the unit of L). A map of this kind is called a *support* on A with values in L (a terminology introduced by Joyal; see also [5]). Now, the radical content trivially satisfies the last three of these conditions while the first is exactly Proposition 1. Hence, the point of the latter is that the radical content is a support on $A[x]$ with values in the (distributive) lattice of (finitely generated) radical ideals of A.

It should be added that all this can be presented in a particularly natural and suggestive way by placing it in an appropriate topos-theoretic context, but that would go rather beyond the scope of the present note [9; 3; 4, Ch.V].

3. Spectral aspects

Here, we relate our result on the radical content to the spectra of A and $A[x]$.

Recall that, classically, the *spectrum* of A is the topological space of all prime ideals $\mathfrak{p}$ of A, with basic open sets $\{\mathfrak{p} \mid a \notin \mathfrak{p}\}$ for each $a \in A$, while any ring homomorphism $h: A \to B$ induces a continuous map between the respective spectra which takes each prime ideal $\mathfrak{p}$ of B to its inverse image $h^{-1}(\mathfrak{p})$, resulting in a contravariant functor from

the category **Ann** of commutative rings with unit to the category **Top** of topological spaces. As is well-known, the usefulness of this functor is closely tied to the nature of the foundation on which **Ann** is based while a less restrictive, and therefore more natural, counterpart is provided by the *localic* notion of spectrum.

For this, **Top** is replaced by the category **Loc** of locales, the formal dual of the category **Frm** of frames, where a frame is a complete lattice L which satisfies the distribution law

$$x \wedge \bigvee S = \bigvee \{x \wedge t \mid t \in S\}$$

for all $x \in L$, $S \subseteq L$, and a frame homomorphism is a map $L \to M$ between frames preserving all finite meets, including the unit e, and arbitrary joins, including the zero 0. We shall adopt the (formally redundant but conceptually suggestive) convention which makes a notational distinction between a frame L and its corresponding locale X, expressing the relation between them by $\mathfrak{O}X = L$; a locale map $f: X \to Y$ is then the same as a frame homomorphism $h: \mathfrak{O}Y \to \mathfrak{O}X$, where this relation is expressed by $h = \mathfrak{O}f$ or, alternatively, $h = f^*$. For basic facts concerning locales, see [4].

Now, the localic spectrum Spec$A$ of any $A \in$ **Ann** is given by the specification $\mathfrak{O}$ (Spec$A$) $= RIdA$, the frame of all radical ideals of A, and for any ring homomorphism $h: A \to B$ the associated locale map Spec$B \to$ Spec$A$ is determined by the frame homomorphism $RIdA \to RIdB$ taking each radical ideal I of A to the radical ideal of B generated by its image $h[I]$. Obviously, this provides a contravariant functor **Ann** $\to$ **Loc**. The classical spectrum results from this localic spectrum by composition with the spectrum functor **Loc** $\to$ **Top**, and hence the localic spectrum is the more basic entity which logically precedes the classical one. On the other hand, $RIdA$ is also the Lindenbaum algebra of the propositional theory of a prime of A [7], and viewed in this light one sees Spec$A$ as the locale of primes of A, while the locale map Spec$B \to$ Spec$A$ induced by a homomorphism $A \to B$ amounts to taking inverse images of primes. Thus, conceptually, the localic spectrum is none other than the classical one, but again lifted to a somewhat different plane.

For any ring extension $B \supseteq A$, the locale map Spec$B \to$ Spec$A$ corresponding to the indentical embedding, determined by the expansion of radical ideals from A to B, will be called the natural map from Spec$B$ to Spec$A$.

Now we have, concerning any A and $A[x]$.

Proposition 2. *The natural map Spec$A[x] \to$ Spec$A$ has a right adjoint right inverse Spec$A \to$ Spec$A[x]$.*

Proof. In the present situation, the frame homomorphism $RIdA \to RIdA[x]$ providing the natural map Spec$A[x] \to$ Spec$A$ takes each radical ideal I in A to the ideal $I[x]$ since the latter is already a radical ideal in $A[x]$ by Corollary 4 of Proposition 1. On the other hand, by general facts concerning supports, the radical content determines a frame homomorphism $k: RIdA[x] \to RIdA$ such that $k([u]) = J(u)$. Then, for

any radical ideal H of $A[x]$, $k(H)$ is the radical ideal of A generated by the coefficents of the $u \in H$, and hence

$$k(H) \subseteq I \text{ iff } H \subseteq I[x] \quad (I \in RIdA)$$

so that k is left adjoint to the natural map $RIdA \to RIdA[x]$. In addition, we obviously have $k(I[x]) = I$, and in all, this proves the proposition. □

Remark. The above result is the localic counterpart, or more precisely, the localic antecedent, of the familiar fact that, for the classical spectra, the continuous map $\mathfrak{P} \rightsquigarrow \mathfrak{P} \cap A$, $\mathfrak{P}$ any prime ideal of $A[x]$, has as continuous right inverse the map $\mathfrak{p} \rightsquigarrow \mathfrak{p}[x]$ which makes the spectrum of A a dense retract of the spectrum of $A[x]$.

4. A general view

It makes sense, for any ring extension $B \supseteq A$, to ask whether the natural map $\mathrm{Spec}B \to \mathrm{Spec}A$ has a right adjoint right inverse. In particular, this question might be considered for the free extension $A[M]$ of A by some commutative monoid M – the polynomial ring over A being the special case where M is the free commutative monoid on one generator.

For a monoid algebra $A[M]$ over A, one has the counterpart of the radical content of a polynomial provided M has decidable equality: this ensures that the notion of coefficient occurring in the representation of u with respect to the A-module basis M of $A[M]$ makes sense, and $J(u)$ may be defined as the radical ideal generated by these.

The following result characterizes those M (with decidable equality) for which the counterpart of Proposition 1 holds. We note that the present conditions on M also describe the M for which $A[M]$ is an integral domain whenever A is [2], which is, however, not surprising since both questions are in fact the same, for the ring extensions involved, when considered at the level of the theory of a prime.

Proposition 3. *The radical content is a support on each $A[M]$ iff M is cancellative and power cancellative.*

Proof. ($\Rightarrow$) If $xz = yz$ in M then $(x - y)z = 0$ in $\mathbb{Q}[M]$ so that

$$J(x - y) \cap J(z) = J(0) = (0)$$

while $J(z) = (1)$. Hence $J(x - y) = (0)$, and this implies $x = y$. Similarly, if $x^n = y^n$ for any $x, y \in M$ and $n > 1$ then, also in $\mathbb{Q}[M]$,

$$0 = (x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}),$$

hence

$$(0) = J(x-y) \cap J(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}) = J(x-y),$$

and thus, again, $x = y$.

($\Leftarrow$) We derive the Lemma, and hence consider $uv = 0$ for $u = a_0 s_0 + \cdots + a_n s_n$ and $v = b_0 t_0 + \cdots + b_m t_m$ in $A[M]$, for semiprime A. Here, we may assume that M is generated by the elements $s_0, \ldots, t_m$. Now, as a cancellative commutative monoid, M is embedded in its group G of fractions while G is torsion-free since M is power cancellative. This makes G a finite product of infinite cyclic groups, say, $G = (x_1)(x_2)\cdots(x_m)$, and there exists $s \in G$ such that su and sv belong to the polynomial ring $A[x_1, \ldots, x_m]$. Since $uv = 0$ implies $(su)(sv) = 0$ it follows that all $a_i b_k = 0$ by the extension of the Lemma to arbitrary polynomial rings. □

The following conditions make natural sense for any given A and M; we add some remarks concerning the relationship between them:

I: Proposition 1,

II: Proposition 2,

III: For any radical ideal I of A, $I[M]$ is a radical ideal of $A[M]$,

IV: The natural frame homomorphism $RIdA \to RIdA[M]$ has a left adjoint.

It is immediate that I implies II and trivial that II implies IV. Also, I implies III since $J(u) \subseteq I$ iff $u \in I[M]$, while III implies IV since the map $I \rightsquigarrow I[M]$ preserves intersections. Finally, II and III implies I: in view of III, the left adjoint $k: RIdA[M] \to RIdA$ to the natural $RIdA \to RIdA[M]$, which is supplied by II, satisfies the condition

$$k(H) \subseteq I \text{ iff } H \subseteq I[M]$$

for any radical ideals H and I of $A[M]$ and A, respectively. This shows that $k([u]) = J(u)$, for any $u \in A[M]$, and since k is a frame homomorphism I follows.

The following examples show that all four implications I $\Rightarrow$ II, III and II, III $\Rightarrow$ IV are strict.

Example 1. III $\not\Rightarrow$ I: Let M be the monoid with two elements, its unit and $x = x^2$. For any A, take $u = a + bx \in A[M]$ such that $u^2 = 0$. Then $a^2 + (2ab + b^2)x = 0$, hence $a^2 = 0 = 2ab + b^2$ which implies $a = 0 = b$ for semiprime A, and by the proof of Corollary 4 of Proposition 1 this proves III. On the other hand, $x(1-x) = 0$ and hence $J(x(1-x)) = [0]$ while $J(x) = (1) = J(1-x)$, showing that I fails. Note that this also shows IV $\not\Rightarrow$ II since III $\Rightarrow$ IV and II & III $\Rightarrow$ I.

Example 2. IV $\not\Rightarrow$ III: For any (geometric) *field* K, $RIdK \to RIdK[M]$ always has a left adjoint, given by the radical content. On the other hand, $(0)[M] = (0)$ need not be a radical ideal in $K[M]$: if K has prime characteristic p and M an element s of order p then $(1-s)^p = 0$ so that $1 - s \neq 0$ belongs to rad(0) in $K[M]$.

Examples 3. II $\not\Rightarrow$ I: For the prime field $\mathbb{F}_2$ and a cyclic group $G = (x)$ of order 2, the only ideal in $\mathbb{F}_2[G]$ besides (0) and (1) is $(1 + x)$ so that $RId\mathbb{F}_2(G]$ consists of $[0] = (1 + x)$ and (1). This makes the natural homomorphism $RId\mathbb{F}_2 \to RId\mathbb{F}_2[G]$ an isomorphism so that II holds trivially. On the other hand, I fails since $(1 + x)^2 = 0$.

We close with a remark of a different kind. Concerning the alternative approach to a general notion of polynomial content used in the Dedekind–Mertens Lemma discussed in the Remark after Proposition 1, one might hope for the identity $I(uv) = I(u) \cap I(v)$ or perhaps $I(uv) = I(u) \cdot I(v)$, but neither holds: If A is an extension of $\mathbb{F}_2$ by elements s and t for which $s^2 = t^2 = 0$ but $st \neq 0$ then, in $A[x]$, $(s + tx)^2 = 0$ while $(s, t) \cdot (s, t) = (st) \neq (0)$.

Acknowledgements

This note was written while B. Banaschewski was visiting the University of Cape Town, June–November 1993. Thanks go to the Categorical Topology Research Group for financial assistance as well as to the Natural Science and Engineering Research Council of Canada for support in the form of a research grant.

References

[1] M.F. Atiyah and I.G. MacDonald, Introduction to Commutative Algebra (Addison-Wesley, Reading, MA, 1969).

[2] B. Banaschewski, On proving the absence of zero–divisors for semigroup rings, Canad. Math. Bull 4 (1961) 225–231.

[3] P.T. Johnstone, Rings, fields and spectra, J. Algebra 49 (1977) 238–260.

[4] P.T. Johnstone, Stone Spaces, Cambridge Studies in Advanced Mathematics, Vol. 3 (Cambridge Univ. Press, Cambridge, 1982).

[5] A. Joyal, Les théorèmes de Chevalley–Tarski et rémarques sur l'algèbre constructive, Cahiers Topologie Géom. Différentielle 16 (1976) 256–258.

[6] F.W. Lawvere, Quantifiers and sheaves, Actes du Congrès Intern. des Math., Nice 1970, tome I (Gautiers–Villars, Paris, 1970) 329–334.

[7] C.J. Mulvey, Synctactic construction of the spectrum of a commutative ring, Tagungsbericht of Oberwolfach Category Meeting, 1974.

[8] D.G. Northcott, A generalization of a theorem on the contents of polynomials, Proc. Cam. Phil. Soc. 55 (1959) 282–288.

[9] M. Tierney, On the spectrum of a ringed topos, in: Algebra, Topology and Category Theory: a collection of papers in honour of Samual Eilenberg (Academic Press, New York, 1976) 189–210.